IN THE CLAIMS:

Please amend the Claims of the above-identified application so as to read as follows:

1. (Currently Amended) An anti-tampering signature method ~~for rewritable media wherein display data displayed on rewritable medium that displays display data stored in a writeable and erasable state is certified, the method~~ comprising the steps of:

providing a rewriteable media including (i) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to said certifier identification areas wherein certification data associated with each certifier is respectively stored in a visually viewable, rewritable and erasable state;

determining whether or not certifier signature information contained in said plurality of display data certifier identification areas, or to be added to one of said display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

~~an extraction step of~~ extracting a characteristic quantity ~~from~~ that represents a characteristic of image data ~~that is~~ generated by reading the display data according to an instruction from a certifier who has certified the display data,

~~a data generation step of~~ generating encrypted data by encrypting ~~the~~ said characteristic quantity using an encryption key paired with an identifier,

~~an~~ appending ~~step of appending~~ ~~the~~ each said identifier and ~~the~~ its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, ~~and~~

~~a judgment step of~~ obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate,

decrypting the obtained characteristic quantity of of the display data, and

judging whether or not the decrypted characteristic quantity obtained by decrypting the encrypted data and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warming that signature tampering may have occurred.

2. (Currently Amended) The anti-tampering signature method ~~for rewritable media~~ according to claim 1, wherein, in the extraction step, a general characteristic extracted from the image data generated by reading the display data is used as the characteristic quantity.

3. (Currently Amended) An anti-tampering signature apparatus for executing an anti-tampering signature method ~~for rewritable media wherein display data displayed on a rewritable medium that displays display data stored in a writeable and erasable state is certified, the apparatus~~ comprising:

a rewriteable media including (i) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to said plurality of display data certifier identification areas wherein certification data associated with each certifier is respectively stored in a visually viewable, rewritable and erasable state;

first tampering judgment means for determining whether or not certifier signature information contained in said plurality of display data certifier identification areas, or to be added to one of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and for in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

~~a~~ characteristic quantity extraction means for extracting a characteristic quantity that represents a characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

~~an~~ encryption / decryption means that generates encrypted data by encrypting ~~the~~ said characteristic quantity using an encryption key paired with an identifier, and decrypts the encrypted data into ~~the~~ said characteristic quantity,

~~an~~ appending means for appending ~~the~~ each said identifier and ~~the~~ its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, and

~~a~~ second-tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.

4. (Currently Amended) An anti-tampering signature system wherein display data is displayed on a rewritable medium ~~that displays display data stored in a writeable and erasable state~~ including (i) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to said plurality of display data certifier identification areas wherein certification data associated with each certifier is respectively stored in a visually viewable, rewritable and erasable state is certified, comprising:

first tampering judgment means for determining whether or not certifier signature information contained in said plurality of display data certifier identification areas, or to be added to one of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and for in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

~~an~~ encryption key generating means that registers an identifier and generates an encryption key,

~~a~~ storage means for storing the identifier and the encryption key,

~~a~~ certifying means that supplies the encryption key according to a query based on the identifier, and

~~an~~ anti-tampering signature apparatus provided with a characteristic quantity extraction means for extracting a characteristic quantity that represents a characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data, ~~an~~ encryption / decryption means that generates encrypted data by encrypting ~~the~~ said characteristic quantity using an encryption key paired with an identifier~~,~~ and decrypts the encrypted data into ~~the~~ said characteristic quantity, ~~an~~ appending means for appending ~~the~~ each said identifier and ~~the~~ its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, and ~~a~~ second tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.

5. Cancelled, without prejudice.

6. (Currently Amended) A computer-readable recording medium on which is stored an anti-tampering signature program for causing a computer to perform an anti-tampering signature method with respect to a rewritable media including (i) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to said certifier identification areas wherein certification data associated with each certifier is respectively stored in a visually viewable, rewritable and erasable state, said anti-tampering signature program comprising the steps of::

determining whether or not certifier signature information contained in said plurality of display data certifier identification areas, or to be added to, one of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

extracting a characteristic quantity that represents a characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

generating encrypted data by encrypting said characteristic quantity using an encryption key paired with an identifier,

appending each said identifier and its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate,

decrypting the obtained characteristic quantity of the display data, and

judging whether or not the decrypted characteristic quantity obtained by decrypting the encrypted data and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.